

**Department of Justice**  
U.S. Attorney's Office  
Northern District of California

FOR IMMEDIATE RELEASE

Wednesday, July 26, 2017

**Russian National And Bitcoin Exchange Charged In 21-Count  
Indictment For Operating Alleged International Money  
Laundering Scheme And Allegedly Laundering Funds From Hack  
Of Mt. Gox**

**Defendant Alexander Vinnik Was Arrested in Greece to Face Charges in the  
United States; Bitcoin Exchange Alleged to Have Received Deposits Valued  
at Over \$4 Billion**

SAN FRANCISCO – A grand jury in the Northern District of California has indicted a Russian national and an organization he allegedly operated, BTC-e, for operating an unlicensed money service business, money laundering, and related crimes. The announcement was made by U.S. Attorney Brian J. Stretch for the Northern District of California; Acting Assistant Attorney General Kenneth A. Blanco of the Justice Department's Criminal Division; Internal Revenue Service (IRS) Criminal Investigation Chief Don Fort; Immigration and Customs Enforcement's (ICE) Homeland Security Investigations (HSI) Acting Executive Associate Director Derek Benner; Federal Bureau of Investigation (FBI) Special Agent in Charge of the Louisville Division Amy Hess; United States Secret Service (USSS) Special Agent in Charge of the Criminal Investigative Division Michael D'Ambrosio; Federal Deposit Insurance Corporation (FDIC), Office of the Inspector General, Inspector General Jay N. Lerner; and Acting Director of the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), Jamal El-Hindi.

"Cryptocurrencies such as Bitcoin provide people around the world new and innovative ways of engaging in legitimate commerce. As this case demonstrates, however, just as new computer technologies continue to change the way we engage each other and experience the world, so too will criminals subvert these new technologies to serve their own nefarious purposes," said U.S. Attorney Stretch. "This office will continue to devote the necessary resources to ensure that money launderers and cyber-criminals are detected, apprehended, and brought to justice wherever and however they use the internet to commit their crimes."

"As this case demonstrates, the Criminal Division employs a multi-faceted approach to dismantling criminal enterprises, by prosecuting the criminal actors themselves, and by shutting down their ability to monetize their crimes through entities that facilitate money laundering," said Acting Assistant Attorney General Blanco. "The Criminal Division will work tirelessly to identify those who

use technology to conduct and obscure their criminal activity, as we ensure there are no safe havens from U.S. justice for those who seek to victimize Americans."

"Homeland Security Investigations is strongly committed to tracking down criminals who seek to strike at the foundations of global financial security through complex money laundering schemes," said HSI Acting Executive Associate Director Derek Benner. "The resulting indictment is a clear representation of why our close law enforcement partnerships are vital to our shared missions. HSI will continue to aggressively target those who deliberately seek to exploit financial systems for personal gain."

"Mr. Vinnik is alleged to have committed and facilitated a wide range of crimes that go far beyond the lack of regulation of the bitcoin exchange he operated. Through his actions, it is alleged that he stole identities, facilitated drug trafficking, and helped to launder criminal proceeds from syndicates around the world," said Chief Don Fort, IRS Criminal Investigation. "Exchanges like this are not only illegal, but they are a breeding ground for stolen identity refund fraud schemes and other types of tax fraud. When there is no regulation and criminals are left unchecked, this scenario is all too common. The takedown of this large virtual currency exchange should send a strong message to cyber-criminals and other unregulated exchanges across the globe."

"BTC-e was noted for its role in numerous ransomware and other cyber-criminal activity; its takedown is a significant accomplishment, and should serve as a reminder of our global reach in combating transnational cyber crime," said Special Agent in Charge of the USSS Criminal Investigative Division Michael D'Ambrosio. "We are grateful for the efforts of our law enforcement partners in achieving this significant result."

"The arrest of Alexander Vinnik is the result of a multi-national effort and clearly displays the benefits of global cooperation among US and international law enforcement," said FBI Special Agent in Charge Hess. "This investigation demonstrates the long-term commitment given to identifying and pursuing criminals world-wide with a whole of government approach. This was a highly complex investigation that has only reached this stage due to the persistent and dedicated efforts of all the parties involved. We must continue to impose real costs on criminals, no matter who they are or where they attempt to hide."

"The Federal Deposit Insurance Corporation Office of Inspector General works to ensure the integrity of the financial service sector and is committed to holding accountable those involved in criminal activity that undermine its integrity," said Inspector General Lerner. "This investigation demonstrates what can be achieved among the cooperative partnerships in the domestic and international law enforcement community."

The indictment describes Alexander Vinnik, 37, a Russian citizen, as the owner and operator of multiple BTC-e accounts, including administrator accounts, and also a primary beneficial owner of BTC-e's managing shell company, Canton Business Corporation. According to the indictment, numerous withdrawals from BTC-e administrator accounts went directly to Vinnik's personal bank accounts. The indictment further alleges that proceeds from well-known hacks and thefts from bitcoin exchanges were funded through a BTC-e administrator account associated with Vinnik. Vinnik was arrested in Greece on July 25.

According to the indictment unsealed today, BTC-e, founded in 2011, was one of the world's largest and most widely used digital currency exchanges. The indictment alleges that BTC-e allowed its users to trade in the digital currency "Bitcoin" with high levels of anonymity. The indictment alleges that although Bitcoin has known legitimate uses, the virtual currency, like cash, can be used to facilitate illicit transactions and to launder criminal proceeds. According to the indictment, since its inception, Vinnik and others developed a customer base for BTC-e that was heavily reliant on criminals, including by not requiring users to validate their identity, obscuring and anonymizing transactions and source of funds, and by lacking any anti-money laundering processes. The indictment alleges BTC-e was operated to facilitate transactions for cybercriminals worldwide and received the criminal proceeds of numerous computer intrusions and hacking incidents, ransomware scams, identity theft schemes, corrupt public officials, and narcotics distribution rings. Thus, the indictment alleges, BTC-e was used to facilitate crimes ranging from computer hacking, to fraud, identity theft, tax refund fraud schemes, public corruption, and drug trafficking. The investigation has revealed that BTC-e received more than \$4 billion worth of bitcoin over the course of its operation.

As to Vinnik, the indictment alleges that he received funds from the infamous computer intrusion or "hack" of Mt. Gox – an earlier digital currency exchange that eventually failed, in part due to losses attributable to hacking. The indictment alleges that Vinnik obtained funds from the hack of Mt. Gox and laundered those funds through various online exchanges, including his own BTC-e and a now defunct digital currency exchange, Tradehill, based in San Francisco, California. The indictment alleges that by moving funds through BTC-e, Vinnik sought to conceal and disguise his connection with the proceeds from the hacking of Mt. Gox and the resulting investigation.

As for defendant BTC-e, the indictment alleges that, despite doing substantial business in the United States, BTC-e was not registered as a money services business with the U.S. Department of the Treasury, had no anti-money laundering process, no system for appropriate "know your customer" or "KYC" verification, and no anti-money laundering program as required by federal law. According to the company's website, BTC-e is located in Bulgaria but organized or otherwise subject to the laws of Cyprus. The exchange allegedly maintains a base of operations in the Seychelles Islands and its

web domains are registered to shell companies in, among other places, Singapore, the British Virgin Islands, France, and New Zealand.

The indictment charges BTC-e and Vinnik with one count of operation of an unlicensed money service business, in violation of 18 U.S.C. § 1960, and one count of conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(h). In addition, the indictment charges Vinnik with seventeen counts of money laundering, in violation of 18 U.S.C. § 1956(a)(1), and two counts of engaging in unlawful monetary transactions, in violation of 18 U.S.C. § 1957. An indictment merely alleges that crimes have been committed, and the defendants are presumed innocent until proven guilty beyond a reasonable doubt.

FinCEN today assessed a \$110 million civil money penalty against BTC-e for willfully violating U.S. anti-money laundering (AML) laws. Alexander Vinnik was assessed \$12 million for his role in the violations.

“We will hold accountable foreign-located money transmitters, including virtual currency exchangers, that do business in the United States when they willfully violate U.S. AML laws,” said Acting FinCEN Director Jamal El-Hindi. “Today’s action should be a strong deterrent to anyone who thinks that they can facilitate ransomware, dark net drug sales, or conduct other illicit activity using encrypted virtual currency. Treasury’s FinCEN team and our law enforcement partners will work with foreign counterparts across the globe to appropriately oversee virtual currency exchangers and administrators who attempt to subvert U.S. law and avoid complying with U.S. AML safeguards.”

If convicted of these crimes, Vinnik faces the following maximum penalties:

<b>Violation</b>	<b>Statute</b>	<b>Maximum Penalty</b>
operation of an unlicensed money service business	18 U.S.C. § 1960	5 years of imprisonment
conspiracy to commit money laundering	18 U.S.C. § 1956(h)	20 years of imprisonment and a \$500,000 fine or twice the value of the property involved in the transaction
money laundering	18 U.S.C. § 1956(a)(1)	20 years of imprisonment and a \$500,000 fine or twice the value of the property involved in the transaction (each count)

engaging in unlawful monetary transactions	18 U.S.C. § 1957	10 years of imprisonment and a \$500,000 fine or twice the value of the property involved in the transaction (each count)
--	------------------	---

Additional fines, restitution, and supervised release also may be ordered. However, any sentence will be imposed by the court only after consideration of the U.S. Sentencing Guidelines and the federal statute governing the imposition of a sentence, 18 U.S.C. § 3553.

This case is being investigated by the Internal Revenue Service (the Oakland Calif., Field Office and Cyber Crime Unit in Washington, D.C.); Department of Homeland Security, Homeland Security Investigations; FBI; U.S. Secret Service Criminal Investigative Division; and Federal Deposit Insurance Corporation, Office of the Inspector General. The case is being prosecuted by the U.S. Attorney's Office for the Northern District of California and the Criminal Division's Computer Crime and Intellectual Property Section. The Criminal Division's Office of International Affairs provided substantial assistance on the case.